

PATENT COOPERATION TREATY

REC'D. 04 FEB 2005

WIPO

PCT

PCT



INTERNATIONAL PRELIMINARY EXAMINATION REPORT
(PCT Article 36 and Rule 70)

Applicant's or agent's file reference IN/PA-210	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/PEA416)	
International application No. PCT/IN 03/00339	International filing date (day/month/year) 20.10.2003	Priority date (day/month/year) 26.10.2002
International Patent Classification (IPC) or both national classification and IPC G09C1/00		
Applicant THE ADDITIONAL DIRECTOR (IPR), DEFENCE ... et al.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 6 sheets, including this cover sheet.
- ☐ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).
- These annexes consist of a total of sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the opinion
- II ☐ Priority
- III ☒ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand 22.05.2004	Date of completion of this report 03.02.2005
Name and mailing address of the international preliminary examining authority:  European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized Officer Cretaine, P Telephone No. +49 89 2399-8828 

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. **PCT/IN 03/00339**

I. Basis of the report

1. With regard to the **elements** of the international application (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17)*):

Description, Pages

1-18 as originally filed

Claims, Numbers

1-11 as originally filed

Drawings, Sheets

1/7-7/7 as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language: , which is:

- ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
- ☐ the claims, Nos.:
- ☐ the drawings, sheets:

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. **PCT/IN 03/00339**

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)).

(Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

6. Additional observations, if necessary:

III. Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

1. The questions whether the claimed invention appears to be novel, to involve an inventive step (to be non-obvious), or to be industrially applicable have not been examined in respect of:

☐ the entire international application,

☒ claims Nos. 11

because:

☐ the said international application, or the said claims Nos. relate to the following subject matter which does not require an international preliminary examination (specify):

☐ the description, claims or drawings (*indicate particular elements below*) or said claims Nos. are so unclear that no meaningful opinion could be formed (*specify*):

☐ the claims, or said claims Nos. are so inadequately supported by the description that no meaningful opinion could be formed.

☒ no international search report has been established for the said claims Nos. 11

2. A meaningful international preliminary examination cannot be carried out due to the failure of the nucleotide and/or amino acid sequence listing to comply with the standard provided for in Annex C of the Administrative Instructions:

☐ the written form has not been furnished or does not comply with the Standard.

☐ the computer readable form has not been furnished or does not comply with the Standard.

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes: Claims	1-10
	No: Claims	
Inventive step (IS)	Yes: Claims	
	No: Claims	1-10
Industrial applicability (IA)	Yes: Claims	1-10
	No: Claims	

2. Citations and explanations

see separate sheet

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/IN 03/00339

Re Item V

**Reasoned statement with regard to novelty, inventive step or industrial applicability;
citations and explanations supporting such statement**

Reference is made to the following documents:

D1 = MENEZES, VANSTONE et al.: "The State of Elliptic Curve Cryptography". Design, Codes and Cryptography, vol.19, pages 173-193, March 2000, Kluwer Academic Publishers, Boston.

D2 = WO-A-94 15423

The document D1 was not cited in the international search report.

1. Independent claim 1:

D1 discloses, according to the essential features of claim 1, a method of elliptic curve encryption ("Elliptic Curve Cryptosystems") comprising the steps of:

- selecting an elliptic curve $E_p(a,b)$ of the form $y^2 = x^3 + ax + b \text{ mod}(p)$ wherein a and b are non-negative integers less than p satisfying the formula $4a^3 + 27b^2 \text{ mod}(p)$ not equal to 0 (D1, page 174, lines 36-41);
- generating a point $G(x,y)$ on the elliptic curve $E_p(a,b)$ ("Q", D1, page 177, lines 15-17)
- generating a private key n_A ("k_A", D1, page 177, lines 24-30)
- generating a public key $P_A(x,y)$ given by the formula $P_A(x,y) = (n_A \cdot G(x,y)) \text{ mod}(p)$ ("k_A·Q", D1, pages 177, lines 27-28)
- encrypting the input message MSG (D1, page 177, line 27-28)
- decrypting the ciphered text (D1, page 177, lines 28-29).

The differences between the subject-matter of claim 1 and the disclosure of D1 are the steps of obtaining $G(x,y)$ from a point $B(x,y)$ on the elliptic curve. These steps are:

- generating a large 160 bits random number by a method of concatenation of a number of smaller random numbers
- converting said large random number into a series of powers of 2^{31}
- converting each coefficient of 2^{31} obtained into a binary series

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/IN 03/00339

- multiplying of binary series obtained with the point $B(x,y)$.

The objective problem solved by these differences is to optimise the processing time for scalar multiplication of a point $B(x,y)$ with a large number. This problem is a well-known one in the field of elliptic curves mathematics and computing algorithms (see for instance D2, page 5, lines 11-17).

The solution proposed in claim 1 of the present application cannot be considered as involving an inventive step (Article 33(3) PCT) for the following reasons:

- concatenating small numbers to generate a larger number is an obvious step for a person skilled in computing algorithms
- representing said large number by a decomposition using as base the number 2^{31} lies within the general design competence of the same skilled person desiring to use the capability of a 32-bit computer
- representing each coefficient (which are per se less than 2^{31}) by a decomposition using as base the number 2 also lies within the general design competence of the same skilled person
- multiplication of binary numbers with a point of an elliptic curve is standard practice in the field of elliptic curve mathematics (see also D1, page 183, lines 11-17).

Therefore claim 1 does not meet the requirements of Article 33(3) PCT.

2. Dependent claims:

The additional features introduced by dependent claims 2-10 relate to details of implementation of the basic features specified by the independent claim 1 to which they are appended. All these features appear to be either basically known or readily derivable from documents D1-D2 or to be common measures in the field of elliptic curve mathematics.

Therefore claims 2-10 do not meet the requirements of Article 33(3) PCT.

Furthermore some of these features (in dependent claims 3-6, 8-9) are formulated in such a way that they may fall under the category of program features, as opposed to method features. In particular formulations like "going to next if true", "returning M as result if

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/IN 03/00339

false", "setting $l = l+1$ ", "returning to step iii", render said claim unclear with respect to the category (Article 6 PCT).